UNDERSTANDING AND BUILDING THREAT MODELS

Tas Giakouminakis
Rapid7
Agenda

- Threat Modeling – The Basics
- Understanding Attackers
- Understanding the Organization
- Building Threat Models
Threat Modeling – The Basics

- Asset
- Software
- Attacker
Threat Modeling – Attackers

- Attacker Motivation
- Common Targets
- Attack Patterns
- Organizational Readiness
Attacker Motivations & Targets

► Assume common threats impact everyone
  ► Mass malware
  ► “Unintentional” insiders

► Gain insight into industry specific threats
  ► ISACs
  ► UK CISP
  ► US CISPA
  ► Vendors

Verizon – 2013 Data Breach Investigations Report
Attack Patterns

**Attack Targeting**
- Opportunistic: 75%
- Targeted: 25%

**The Inevitability of the Click**
- Probability of at least one click:
  - 100%
  - 80%
  - 60%
  - 40%
  - 20%
  - 0%

**Difficulty Of Initial Compromise**
- Very Low: 10%
- Low: 22%
- Moderate: 68%
- High: <1%

**Difficulty Of Subsequent Actions**
- Very Low: 12%
- Low: 7%
- Moderate: 21%
- High: 71%

Verizon – 2013 Data Breach Investigations Report
Public Exploit Targets

Rapid7 Metasploit Framework Exploit Contributions through May 3, 2013
Mass Malware Targets

- Mass malware leverages Exploit (Crime) packs
- 49 Exploit (Crime) Packs Analyzed 2011 - 2013

Unique Vulnerabilities Exploited

- Windows Media Player, 1
- Office, 2
- Window, 2
- Firefox, 4
- Reader, 11
- Flash, 12
- IE, 15
- Java, 22

Exploit Packs Per App

- Windows Media Player, 2
- Office, 2
- Window, 8
- Firefox, 2
- Reader, 29
- Flash, 14
- IE, 35
- Java, 46

Contagio Malware Dump & Exploit Intelligence Project/Dan Guido
User Targeted Attacks

- Browse Internet
- Click E-mail Link (Social Engineering)
- Open E-mail Attachment (Social Engineering)
- Open file USB drive (Social Engineering)

Malicious Page (Drive-by, Watering Hole)

Compromised

Acquire Desired Target/Data

Figure 21: Variety of malware actions

<table>
<thead>
<tr>
<th>Type</th>
<th>Financial</th>
<th>Espionage</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware/Keylogger</td>
<td>75%</td>
<td>66%</td>
<td></td>
</tr>
<tr>
<td>Backdoor</td>
<td>63%</td>
<td>63%</td>
<td></td>
</tr>
<tr>
<td>Export data</td>
<td>55%</td>
<td>55%</td>
<td></td>
</tr>
<tr>
<td>Capture stored data</td>
<td>51%</td>
<td>51%</td>
<td></td>
</tr>
<tr>
<td>C2</td>
<td>45%</td>
<td>45%</td>
<td></td>
</tr>
<tr>
<td>Downloader</td>
<td>39%</td>
<td>39%</td>
<td></td>
</tr>
<tr>
<td>Password dumper</td>
<td>18%</td>
<td>18%</td>
<td></td>
</tr>
<tr>
<td>Rootkit</td>
<td>17%</td>
<td>17%</td>
<td></td>
</tr>
<tr>
<td>Adminware</td>
<td>9%</td>
<td>9%</td>
<td></td>
</tr>
<tr>
<td>RAM scraper</td>
<td>4%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>Disable controls</td>
<td>4%</td>
<td>4%</td>
<td></td>
</tr>
<tr>
<td>Capture app data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client-side attack</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verizon – 2013 Data Breach Investigations Report
Social engineering (e.g., spear-phishing) common in APT, targeted and mass malware scenarios.

Users will click on links.

How do we protect them?
Similarities in Attacks

Malware - Powered by compromised/abused web servers & web applications (eg: SQLi, RFI, brute force)

Drive-by downloads provide high yield for mass malware

Watering holes used in APT and targeted attacks

How do you avoid being part of the delivery network?
Understanding the Organization

Visibility

► Correlate attacker motivations with business functions
  ► Look outside as well – who relies upon you?
► Identify potential targets & existing countermeasures
  ► Compile complete inventory of users, assets, software, services and security controls across physical, virtual, VPN, wireless, cloud services and mobile
  ► Classify assets & data
► Associate users with assets they own or access
Understanding the Organization

► Baseline the IT & user environments
  ► Review inventory to identify outliers, gaps & appropriateness

► Baseline user behavior
  ► Review assets users access or own for appropriateness & access patterns

► Baseline “normal” data flows

► Investigate unknowns & anomalies

► Be prepared for false positives / spurious anomalies
Understanding the Organization

- Business continuity requires effective security response
- Response will vary based on threat / attacker motivation
  - Understanding is key to taking appropriate action
- Staff & train resources accordingly to maximize identification & response capabilities
Taking Action

- Significant progress can be made
- Focus efforts on highest return
  - Increase complexity/cost to the attacker
- Be prepared – easier to contain incidents through planned response than reactive scrambling
Building Threat Models

Let’s work through a few examples

Threat 1: Users will click on links

Threat 2: Serving Malware on the web
Threat: Users Will Click on Links

Motivation
All – Opportunistic through APT

Target
All

Attack Pattern
E-mail, Malware & Actions

Readiness
Varies
Analyzing The Threat

- User
  - User awareness training

- Click E-mail Link
  - Sender ID/SPF, content filtering, …

- Malicious Page
  - URL reputation, content filtering, AV, …

- Compromised
  - Patch software, exploit mitigations, HIDS/HIPS, …

- TBD installed
  - AV, HIDS/HIPS, UAC, limit admin privileges, …

- TBD action
  - App whitelist, egress filters, DLP, IDS, blacklist, …
Reduce Exploit Exposure

► Automate deployment of software, patches, security controls & configurations
► Remove or patch commonly targeted applications
► Limit administrative privileges, User Account Control (UAC)
► Enable exploit mitigations
  ► DEP, ASLR, EMET, SEHOP
► Endpoint security controls
  ► Application whitelisting, AV, FW, IPS

1) Source: National Vulnerability Database
2) Source: ExploitDB
3) Source: Contagio Dump, Exploit Packs 2011 - 2013
Control Traffic Flow

► Gain visibility & increase defensive/response capabilities

► Consolidate ingress & egress points – including VPN & Cloud Services

► Perimeter doesn’t exist – apply security controls closest to resources

► Centralized & consistent logging for network services and security controls
  ► Network services: DNS, FW, VPN, Web, Email, File, Directory, Database
  ► Security controls: IDS/IPS, DLP, WAF, Malware Protection, etc
Limit the Temptations

- Rollout user awareness training, tips & advice
- Reduce spear phishing attacks – leverage Sender ID or Sender Policy Framework (SPF)
- Deploy network-based security controls
  - Blacklist, Malware Protection, IDS/IPS, Content Filtering
Practice & Refine

- Automate social engineering campaigns
- Focus on real-world scenarios, not simulations
- Quantify user susceptibility
- Review security response for lessons learned
  - Failed controls, monitors, or people?
  - Appropriate parties in response chain?
  - Timely and accurate response?
- Refine & iterate
Threat: Serving Malware on the Web

- **Motivation**: All – Opportunistic through APT
- **Target**: All
- **Attack Pattern**: Compromise Web Server, Serve Malware
- **Readiness**: Varies
Analyzing The Threat

- **Bad Actor**: Blacklist (unlikely)
- **Web Server**: Patch software, WAF, IDS/IPS
- **SQL Injection**: Patch software, WAF, IDS/IPS, secure coding
- **Serve Malicious Page**: Secure coding
- **User Compromised**: Refer to Threat 1: Users Will Click on Links
Reduce Exploit Exposure

- Identify all web servers & applications
  - Perform static and dynamic analysis of web applications
- Train developers on secure coding practices
  - OWASP
  - Don’t forget output validation!
- Deploy security controls: WAF, IDS/IPS
- Automate deployment of software, patches, security controls & configurations
Centralized & consistent logging for network services and security controls

- Network services: DNS, FW, VPN, Web, Email, File, Directory, Database
- Security controls: IDS/IPS, DLP, WAF, Malware Protection, etc

Compare dynamic website analysis against baseline for unexpected links
Practice & Refine

► Perform SQL injection attacks
► Focus on real-world scenarios, not simulations
► Review security response for lessons learned
  ► Failed controls, monitors, or people?
  ► Appropriate parties in response chain?
  ► Timely and accurate response?
► Refine & iterate
Additional Reading – Methodologies

Intel Threat Agent Risk Assessment (TARA)
  http://communities.intel.com/docs/DOC-4693

Factor Analysis of Information Risk (FAIR)
  https://www2.opengroup.org/ogs/jsp/publications/PublicationDetails.jsp?publicationid=12239

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM)
  http://www.cert.org/octave/

NIST Risk Management Framework (RMF)

OWASP Threat Risk Modeling
  https://www.owasp.org/index.php/Threat_Risk_Modeling
Additional Reading – Related Works

Lockheed Martin Corp. - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

Dan Guido – Exploit Intelligence Project
   http://www.trailofbits.com/resources/exploit_intelligence_project_2_slides.pdf

Dino Dai Zovi – Attacker Math 101

Australian DSD – Strategies to Mitigate Targeted Cyber Intrusions

SANS/CSIS – Twenty Critical Security Controls for Effective Cyber Defense
   http://www.sans.org/critical-security-controls/
Final Thoughts

- Enhance & maintain visibility into your business, your IT environment, your users, & the threats you face
  - Visibility is key to informed decision making

- Continuously refine your hypotheses & approach, adjust course as needed & validate your results
  - Attacks will continue to evolve – repeat this process frequently
  - Focus efforts on highest return – make attackers work harder

- Operationalize & optimize programs & processes to enable efficiency & effectiveness
  - Human resources as well, not just technology
Thank You

Tas Giakouminakis
Rapid7
Co-founder & Chief Technology Officer
www.rapid7.com
tas@rapid7.com